NISTIR 4934

Protocol Implementation Conformance Statement (PICS) Proforma for the SDNS Security Protocol at Layer 4 (SP4)

Wayne A. Jansen

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Office of Weights and Measures
Gaithersburg, MD 20899

NIST

NISTIR 4934

Protocol Implementation Conformance Statement (PICS) Proforma for the SDNS Security Protocol at Layer 4 (SP4)

Wayne A. Jansen

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Office of Weights and Measures
Gaithersburg, MD 20899

October 1992

U.S. DEPARTMENT OF COMMERCE
Barbara Hackman Franklin, Secretary

TECHNOLOGY ADMINISTRATION
Robert M. White, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

TABLE OF CONTENTS

ABSTRACT

The Secure Data Network System (SDNS) project, initiated by the National Security Agency in 1986, produced a computer network security architecture within the framework of the International Organization for Standardization (ISO) reference model for Open Systems Interconnection (OSI). The security protocol at layer 4 (SP4) is one element of the SDNS architecture used to provide security services at the Transport Layer of the OSI reference model. This report specifies the Protocol Implementation Conformance Statement (PICS) proforma for SP4. When the PICS proforma is completed for an SP4 implementation, it provides a clear and concise statement of capabilities, useful in a variety of situations to those involved in the production, testing, supply, procurement, and application of the implementation.

Key Words: Secure Data Network System; Security Protocol; Protocol Implementation Conformance Statement; Computer Network Security; Open Systems Interconnection;

1. INTRODUCTION

1.1 Background

The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) initiated a joint project in Computer Network Security in 1984. The project was based on the recognition that a comprehensive set of security mechanisms is needed to provide cost effective access control to data in geographically distributed computer networks. While the detailed security mechanisms can differ between the classified and unclassified communities requiring security, both communities benefit when commercial computer networks are developed with a common security architecture. The NSA initiated the Secure Data Network System (SDNS) program in 1986 as a result, at least partially, of this joint project.

Security Protocol 4 (SP4) [1,2] is one element of the SDNS architecture [3], used to provide security services at the Transport Layer of the International Organization for Standardization (ISO) Basic Reference Model (BRM) for Open System Interconnection (OSI) [4]. SP4 consists of a simple encapsulation/decapsulation protocol that protects normal Transport Protocol data units within a cryptographically secure envelope. SP4 is compliant with the security addendum to the OSI BRM [5], and forms the basis of the emerging ISO standard for a Transport Layer Security Protocol [6]. SP4 extends the OSI Transport connectionless and connection oriented standards [7,8] to provide or support the following security services defined in the security addendum:

(1) Data Integrity,

(2) Data Confidentiality,

(3) Data Origination Authentication, and

(4) Access Control.

1.2 Objectives

This report specifies the Protocol Implementation Conformance Statement (PICS) proforma for SP4. The supplier of a protocol implementation which is claimed to conform to the SDNS Standard [1] shall complete the SP4 PICS proforma. A completed PICS proforma becomes the PICS for the implementation in question. The PICS is a statement identifying the capabilities and options of the protocol that have been implemented. The PICS can serve a number of purposes, including as:

(1) a check list for the protocol implementer, to reduce the risk of failure to conform to the standard through oversight;

(2) a detailed indication for the supplier and receiver of the implementation of its capabilities, stated relative to the common basis of understanding provided by the standard PICS proforma;

(3) a basis for the user of the implementation to check the possibility of interworking with another implementation;

(4) the basis for a protocol tester to select appropriate tests against which to assess the claim for conformance of the implementation.

The remainder of this report defines the procedures, format, and content that comprise the SP4 PICS proforma. The format is intended to follow the style used in the PICS proforma for the transport protocol [9]. Most of the content is derived directly from the SP4 standard [1]. Appendix A provides the rationale behind the content selection and explores the relationships between services, protocol, and functions.

2. INSTRUCTIONS

The first part of the PICS proforma, the Implementation Identification, is to be completed as indicated with the information necessary to identify fully both the supplier and the implementation. The main part of the PICS proforma is a fixed-format questionnaire divided into subclauses, each containing a group of individual items. Answers to the questionnaire items are to be provided in the rightmost column, either by simply marking an answer to indicate a restricted choice (usually "Yes" or "No"), or by entering a value or a set or range of values. Note that there are some items where two or more choices from a set of possible answers can apply. Therefore, all relevant choices are to be marked.

Each item is identified by an reference index in the first column; the second column contains the item to be addressed; the third column contains the reference(s) to the location of the item in the main body of the standard. For optional items, additional columns indicate the status of the item (i.e., whether support is optional, or conditional), and the degree of support for the item (i.e., either a Yes/No indication of support, or space to specify implementation support details).

The following standard PICS proforma notations [10] appear in the status column:

Symbol	Meaning
m	mandatory
o	optional
-	not applicable (N/A)
o.<n>	optional, but support of at least one of the group of options labelled by the same numeral <n> is required

Symbol	Meaning (continued)
<cid>:	conditional requirement, according to the condition or item index identified by <cid>
<item>::	simple predicate condition, dependent on the support marked for <item>

3. IDENTIFICATION

Table 1 provides the format for identifying the implementation and its supplier. Only the first three items are required for each implementation. Other information may be completed as appropriate in meeting the requirements for full identification. The terms "Name" and "Version" should be interpreted appropriately to correspond with a supplier's terminology (e.g., using Type, Series, Model).

Table 1: SP4 Implementation Identification

Item	Information
Supplier	_____
Contact point for queries about this PICS	_____
Implementation Name(s) and Version(s)	_____
Other information necessary for full identification (e.g., Name's and Version(s) for machines and operating systems, System Name(s))	_____

4. GENERAL STATEMENT OF CONFORMANCE

Table 2 that follows codifies the general statement of conformance for the implementation.

Table 2: General Conformance Statement

Index	Item	Support	
COTP	Does the implementation claim conformance with ISO/IEC 8073?	Y	N
COMAN	Are all mandatory features of ISO/IEC 8073 implemented?	Y	N
CLTP	Does the implementation claim conformance with ISO/IEC 8602?	Y	N
CLMAN	Are all mandatory features of ISO/IEC 8602 implemented?	Y	N
SP	Does the implementation claim conformance with SDN-401?	Y	N
SPMAN	Are all mandatory features of SDN-401 implemented?	Y	N

5. PROTOCOL IMPLEMENTATION

Table 3 identifies the classes of the connection oriented Transport Protocol (COTP::) supported by the implementation, with regard to their use with either a connection oriented network service (CONS) or a connectionless network service (CLNS).

Table 3: COTP Classes Implemented

Index	Transport Class	Support	
C0	Class 0 SP4-CONS	Y	N
C1	Class 1 SP4-CONS	Y	N
C2	Class 2 SP4-CONS	Y	N
C3	Class 3 SP4-CONS	Y	N
C4	Class 4 SP4-CONS	Y	N
C4L	Class 4 SP4-CLNS	Y	N

6. SECURITY SERVICES SUPPORTED

The following set of tables, 4 through 6, identify for each class of the connection oriented Transport Protocol (COTP::), the security services available through SP4 and their level of support by the implementation. The security services listed are taken from the security addendum to the OSI BRM [2].

Table 4: Service Element Proforma for C0

Index	Service Element	Status	Support	
T0SE0	Confidentiality	o.1	Y	N
T0SE1	Connection Confidentiality	T0SE0:m	Y	N
T0SE2	Connectionless Confidentiality	-		
T0SE3	Integrity	o.1	Y	N
T0SE4	Connection Integrity w Recovery	-		
T0SE5	Connection Integrity wo Recovery	-		
T0SE6	Connectionless Integrity	T0SE3:m	Y	N
T0SE7	Data Origination Authentication	m	Y	N
T0SE8	Access Control	o	Y	N

Table 5: Service Element Proforma for C1, C2, C3

Index	Service Element	Status	Support	
T3SE0	Confidentiality	o.1	Y	N
T3SE1	Connection Confidentiality	T3SE0:m	Y	N
T3SE2	Connectionless Confidentiality	-		
T3SE3	Integrity	o.1	Y	N
T3SE4	Connection Integrity w Recovery	-		
T3SE5	Connection Integrity wo Recovery	T3SE3:o.2	Y	N
T3SE6	Connectionless Integrity	T3SE3:o.2	Y	N
T3SE7	Data Origination Authentication	m	Y	N
T3SE8	Access Control	o	Y	N

Table 6: Service Element Proforma for C4, C4L

Index	Service Element	Status	Support	
T4SE0	Confidentiality	o.1	Y	N
T4SE1	Connection Confidentiality	T4SE0:m	Y	N
T4SE2	Connectionless Confidentiality	-		
T4SE3	Integrity	o.1	Y	N
T4SE4	Connection Integrity w Recovery	T4SE3:o.2	Y	N
T4SE5	Connection Integrity wo Recovery	-		
T4SE6	Connectionless Integrity	T4SE3:o.2	Y	N
T4SE7	Data Origination Authentication	m	Y	N
T4SE8	Access Control	o	Y	N

The following table identifies, for the connectionless Transport Protocol (CLTP::), the security services available through SP4 and their level of support by the implementation.

Table 7: Service Element Proforma for CLTP

Index	Service Element	Status	Support	
TLSE0	Confidentiality	o.1	Y	N
TLSE1	Connection Confidentiality	-		
TLSE2	Connectionless Confidentiality	TLSE0:m	Y	N
TLSE3	Integrity	o.1	Y	N
TLSE4	Connection Integrity w Recovery	-		
TLSE5	Connection Integrity wo Recovery	-		
TLSE6	Connectionless Integrity	TLSE3:m	Y	N
TLSE7	Data Origination Authentication	m	Y	N
TLSE8	Access Control	o	Y	N

7. SUPPORTED FUNCTIONS

The following set of tables, 8 through 13, identify the mandatory and optional functions implemented for each class of Transport (COTP::) supported.

Table 8: Mandatory Functions for C0

Index	Function	Ref
T0F1	verification of peer address	6.4
T0F2	reflection detection	6.3.2
T0F3	security encapsulation	5.5
T0F4	reporting of security events	Notes

Table 9: Optional Functions for C0

Index	Function	Ref	Status	Support	
T0F5	data encipherment	6.2	o.1	Y	N
T0F6	integrity protection	6.3	o.1	Y	N
T0F7	padding	6.6	o	Y	N
T0F8	explicit security labeling	6.5	o	Y	N

Table 10: Mandatory Functions for C1

Index	Function	Ref
T1F1	verification of peer address	6.4
T1F2	reflection detection	6.3.2
T1F3	separation after decapsulation	6.1
T1F4	security encapsulation	5.5
T1F5	reporting of security events	Notes

Table 11: Optional Functions for C1

Index	Function	Ref	Status	Support	
T1F6	data encipherment	6.2	o.1	Y	N
T1F7	integrity protection	6.3	o.1	Y	N
T1F8	pre-encapsulation concatenation	6.1	o	Y	N
T1F9	padding	6.6	o	Y	N
T1F10	explicit security labeling	6.5	o	Y	N

Table 12: Mandatory Functions for C2, C3, C4, C4L

Index	Function	Ref
T4F1	verification of peer address	6.4
T4F2	reflection detection	6.3.2
T4F3	separation after decapsulation	6.1
T4F4	secure multiplexing	Implicit
T4F5	security encapsulation	5.5
T4F6	reporting of security events	Notes

Table 13: Optional Functions for C2, C3, C4, C4L

Index	Function	Ref	Status	Support	
T4F7	data encipherment	6.2	o.1	Y	N
T4F8	integrity protection	6.3	o.1	Y	N
T4F9	integrity sequence number	6.3.3	o	Y	N
T4F10	pre-encapsulation concatenation	6.1	o	Y	N
T4F11	padding	6.6	o	Y	N
T4F12	explicit security labeling	6.5	o	Y	N
T4F13	final sequence number check	6.3.3	o	Y	N

Tables 14 and 15 identify the mandatory and optional functions implemented for the connectionless Transport Protocol (CLTP::).

Table 14: Mandatory Functions for CLTP

Index	Function	Ref
TLF1	verification of peer address	6.4
TLF2	reflection detection	6.3.2
TLF3	security encapsulation	5.5
TLF4	reporting of security events	Notes

Table 15: Optional Functions for CLTP

Index	Function	Ref	Status	Support	
TLF5	data encipherment	6.2	o.1	Y	N
TLF6	integrity protection	6.3	o.1	Y	N
TLF7	padding	6.6	o	Y	N
TLF8	explicit security labeling	6.5	o	Y	N

8. SUPPORTED PROTOCOL DATA UNITS (PDUs)

8.1 Supported Transport PDUs (TPDUs)

As indicated in Table 16, the security encapsulation (SE) TPDU is supported for both transmission and receipt, for the connectionless Transport Protocol (CLTP::) and all classes of the connection oriented (COTP::).

Table 16: TPDUs Supported

Index	TPDU	Item	Status
ST1	SE	transmission	COTP or CLTP:m
ST2	SE	receipt	COTP or CLTP:m

8.2 Supported Parameters of TPDUs

Tables 17 and 18 indicate which parameters are mandatory or optional when a SE TPDU is issued by Transport (COTP:: or CLTP::).

Table 17: Mandatory Parameters for COTP, CLTP

Index	Parameter	Ref
SPI1	Key Identifier must be present.	6.2,6.3
SPI2	Bit one of Protected Header Flag must be set as direction indicator.	8.2.2.2

Table 18: Optional Parameters for COTP, CLTP

Index	Parameter	Ref	Status	Support	
SPI3	Label	8.2.2	o	Y	N
SPI4	Pad	8.2.2	o	Y	N
SPI5	FSN	8.2.3	o	Y	N
SPI6	ICV	8.2.4	o	Y	N

Transport implementations (COTP:: or CLTP::) shall be capable of receiving and processing all possible parameters of the SE TPDU as indicated in Table 19.

Table 19: Mandatory Parameters for COTP, CLTP

Index	Parameter	Ref
SPR1	Key Identifier must be present.	6.2,6.3
SPR2	Bit one of Protected Header Flag must be set as direction indicator.	8.2.2.2
SPR3	Label	8.2.2
SPR4	Pad	8.2.2
SPR5	FSN	8.2.2
SPR6	ICV	8.2.4

8.3 Allowed Values of TPDU Parameters

The following tables indicate the allowed range of values or size of value representation for the parameters of issued or received TPDUs, for the connectionless Transport Protocol (CLTP::) and all classes of the connection oriented (COTP::).

Table 20: Values for Parameters of Issued TPDUs for COTP, CLTP

Index	Parameter	Values	
		Allowed	Supported
AVI1	Key Identifier	1-254 octets	_____
AVI2	Prot Header Flags	"0" or "1"	_____
	Label		
AVI3	Defining Authority	1 octet	_____
AVI4	Value	1-m octets	_____
	Padding		
AVI5	Length	"1" to "254"	_____
AVI6	Value	1-254 octets	_____
AVI7	ICV	1-indef octets	_____

Table 21: Values for Parameters of Received TPDUs for COTP, CLTP

Index	Parameter	Values	
		Allowed	Supported
AVR1	Key Identifier	1-254 octets	_____
AVR2	Prot Header Flags	"0" or "1"	_____
	Label		
AVR3	Defining Authority	1 octet	_____
AVR4	Value	1-m octets	_____
	Padding		
AVR5	Length	"1" to "254"	_____
AVR6	Value	1-254 octets	_____
AVR7	ICV	1-indef octets	_____

Note: Field sizes for the parameters of the protected header must meet the following length restrictions for TPDUs issued and received: 20 + (m+2) + (Length+2) <= 254 octets.

9. SUPPORTED ALGORITHMS

Table 22 identifies the set of confidentiality and integrity algorithms supported by the implementation.

Table 22: Supported Algorithms

Index	Item	Ref	Algorithm Identifier(s)
ALG1	Data Encryption	6.2.3	_____
ALG2	MAC ICV	6.3.1.3	_____
ALG3	MDC ICV	6.3.1.3	_____

10. ERROR HANDLING

10.1 Security Errors

Tables 23 and 24 contain the mandatory and optional security error actions to be taken upon receipt of an SE TPDU corresponding to the event description. In addition, all mandatory actions require that the security relevant event be reported to systems management.

Table 23: Mandatory Security Error Actions for COTP, CLTP

Index	Event	Ref
SER1	An improperly protected TPDU received shall be discarded.	6.0
SER2	A TPDU with an invalid key identifier shall be discarded.	6.2.3
SER3	A TPDU with an invalid ICV shall be discarded.	6.3.1.3
SER4	A TPDU with an invalid direction indicator shall be discarded.	6.3.2.3
SER5	A TPDU with an improper label shall be discarded.	6.5.3
SER6	A TPDU with an improper pad shall be discarded.	6.2.3
SER7	A TPDU with a duplicate sequence number shall be discarded.	6.3.3.1.2
SER8	A TPDU with an invalid peer address shall be discarded.	6.4

Notes: a) In item SER1, an improperly protected TPDU includes both those SE TPDUs where non-negotiated options are used, and those where negotiated options are not used.

b) Item SER7 applies only to the connection oriented Transport Protocol (COTP::) when integrity sequence number space and truncation protection have been negotiated for C2, C3, C4, or C4L.

Table 24: Optional Security Error Actions for COTP, CLTP

Index	Event	Ref	Action	
			Allowed	Supported
SER9	An invalid final sequence number detected for an encapsulated DR, DC, or ER TPDU.	6.3.3.2.3	Local Matter; Audit Advised.	_____
SER10	An invalid destination address, inconsistent with that negotiated for the associated key identifier, appears on an encapsulated TPDU.	None	Open	_____

Note: Item SER9 applies only to the connection oriented Transport Protocol (COTP::) when integrity sequence number space and truncation protection have been negotiated for C2, C3, C4, C4L.

10.2 Protocol Errors

Table 25 identifies the protocol error actions to be taken upon receipt of an SE TPDU corresponding to the event description.

Table 25: Protocol Error Actions for COTP, CLTP

Index	Event	Ref	Action	
			Allowed	Supported
PER1	An undefined parameter encountered in the protected header.	None	Open	_____
PER2	Protected header parameters discovered out of sequence.	None	Open	_____
PER3	FSN parameter appears in the protected header of an encapsulated TPDU, other than DR, DC, or ER.	None	Open	_____

REFERENCES

[1] Specification SDN.401, Secure Data Network Systems (SDNS) Security Protocol 4 (SP4), revision 1.3, National Security Agency, May 1989.

[2] D. Branstad and others, SP4: A Transport Encapsulation Security Protocol, Proceedings National Computer Security Conference, Sept. 1987.

[3] R. Nelson, SDNS Services and Architecture, Proceedings National Computer Security Conference, Sept. 1987.

[4] ISO IS 7498, Open systems Interconnection - Basic Reference Model, 1984.

[5] ISO IS 7498/2, Open Systems Interconnection Reference Model - Security Architecture, 1988.

[6] ISO/IEC DIS 10736, Draft International Standard - OSI Transport Layer Security Protocol, October 11, 1991.

[7] ISO IS 8602, Information Processing Systems - Open Systems Interconnection - Protocol for Providing the Connectionless Mode Transport Service, 1987.

[8] ISO IS 8073, Information Processing Systems - Open Systems Interconnection - Connection Oriented Transport Protocol Specification, 1988.

[9] ISO/IEC JTC 1/SC6 N5839, Third Revised Text of ISO/IEC 8073 PDAD 3.2: Connection Oriented Transport Protocol Specification - Addendum 3: Protocol Implementation Conformance Statement Proforma, July 3 1990.

[10] ISO/IEC JTC 1/SC6 N6233, Catalogue of PICS Proforma Notations, October 15, 1990.

APPENDIX A: SERVICE, FUNCTION, AND PROTOCOL RELATIONSHIPS

The SP4 standard poses a bit of a paradox. Its presentation is simple, yet a high degree of complexity arises when considering its use with the connectionless Transport protocol and the various classes of the connection oriented Transport protocol, in light of the available options. This complexity becomes more evident in the PICS proforma, since the full capabilities of the protocol must be expressed. Perhaps the hardest area of the proforma to reconcile is the SP4 service elements. This is due in large part to the somewhat weak service elements definitions appearing in the security addendum to the OSI reference model. The following guidelines are provided as an aid to understanding:

(1) Connection confidentiality is indicated when the Transport service is connection oriented and the TPDUs are protected accordingly.

(2) Connectionless confidentiality is indicated when the Transport service is connectionless and the TPDUs are protected accordingly.

(3) Connection integrity is indicated when the Transport service is connection oriented, and the integrity sequence number space and per connection key granularity options are in effect. If recovery procedures are included in the Transport class then connection integrity with recovery applies.

(4) Connectionless integrity is indicated when either
   (a) the Transport service is connectionless, or
   (b) the Transport service is connection oriented, the integrity sequence number space option is not in effect, and the per end-system key granularity option is in effect.

(5) Data origination authentication is implicit since a pair-wise key shared between entities is used to decrypt or verify the integrity check value on an incoming security encapsulated TPDU.

(6) Access control is indicated whenever security labels are employed and/or other access controls associated with the cryptographic association have been implemented.

Once the service elements have been resolved, the remainder of the PICS proforma is easier to digest. In particular, the underlying support functions and protocol may be mapped directly from the SP4 security services. The following sections explain these relationships in detail.

A.1 Relationship Between Services and Functions

Table 26 below gives a mapping between OSI security services provided by SP4 and the associated functions needed in an implementation. The consistency between supported functions and security services shall be maintained accordingly.

Table 26: Mapping of Security Services to Supported Functions

Security Service	Functions
Confidentiality	data encipherment padding
Connection Integrity	integrity sequence number space integrity protection reflection detection final sequence number check padding
Connectionless Integrity	integrity protection reflection detection padding
Data Orig. Authentication	verification of peer address security encapsulation use of either: integrity protection or data encipherment
Access Control	explicit security labeling secure multiplexing security encapsulation

A.2 Relationship Between Services and Protocol

Table 27 gives a mapping between OSI security services provided by SP4 and the SE TPDU protocol control information (PCI) and parameter fields employed by the underlying security mechanisms. The consistency between supported security parameters and SE TPDU parameter fields shall be maintained accordingly.

Table 27: Mapping of Security Services to SE TPDU Parameters

Security Service	TPDU Parameters/PCI
Confidentiality	encrypted data pad
Connectionless Integrity	integrity check value direction indicator pad
Connection Integrity	integrity check value direction indicator DT/ED send sequence number final sequence number pad
Data Orig. Authentication	peer address key identifier key identifier employed in: integrity check value or encrypted data
Access Control	security label key identifier key identifier employed in: integrity check value or encrypted data

NIST-114A
(REV. 3-90)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION OR REPORT NUMBER
NISTIR 4934

2. PERFORMING ORGANIZATION REPORT NUMBER

3. PUBLICATION DATE
OCTOBER 1992

4. TITLE AND SUBTITLE

Protocol Implementation Conformance Statement (PICS) Proforma for the SDNS Security Protocol at Layer 4 (SP4)

5. AUTHOR(S)

Wayne A. Jansen

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899

7. CONTRACT/GRANT NUMBER

8. TYPE OF REPORT AND PERIOD COVERED

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)

National Institute of Standards and Technology
Computer Systems Laboratory
Computer Security Division
Gaithersburg, MD 20899

10. SUPPLEMENTARY NOTES

11. ABSTRACT (A 200-WORD OR LESS FACTUAL SUMMARY OF MOST SIGNIFICANT INFORMATION. IF DOCUMENT INCLUDES A SIGNIFICANT BIBLIOGRAPHY OR LITERATURE SURVEY, MENTION IT HERE.)

The Secure Data Network System (SDNS) project, initiated by the National Security Agency in 1986, produced a computer network security architecture within the framework of the International Organization for Standardization (ISO) reference model for Open Systems Interconnection (OSI). The security protocol at layer 4 (SP4) is one element of the SDNS architecture used to provide security services at the Transport Layer of the OSI reference model. This report specifies the Protocol Implementation Conformance Statement (PICS) proforma for SP4. When the PICS proforma is completed for an SP4 implementation, it provides a clear and concise statement of capabilities, useful in a variety of situations to those involved in the production, testing, supply, procurement, and application of the implementation.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)

Computer Network Security; Open Systems Interconnection; Protocol Implementation Conformance Statement; Secure Data Network System; Security Protocol

13. AVAILABILITY

[X] UNLIMITED

[ ] FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).

[ ] ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, DC 20402.

[X] ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES
23

15. PRICE
A02

ELECTRONIC FORM